

Case Study



IronPort Provides Analysis and Management to Enforce Organizational Policies for a Leading Financial Institution

OVERVIEW

Serving 450,000 members, EBS Building Society provides a comprehensive range of financial services including mortgages, savings and investments, pensions, personal loans, credit cards and insurance. The Dublin-based organization operates through a network of offices across Ireland.

EBS places a premium on the trust it has earned through its many years in business. It has also been recognized as one of Ireland's top places to work. With an eye on sustaining its market appeal and the loyalty of its more than 600 employees, the company turned to IronPort to provide it with robust protection against a rising tide of illicit images and content.

EBS BUILDING SOCIETY AT-A-GLANCE

Headquarters: Dublin, Ireland

Business: Mutually-held financial institution that provides mortgages, insurance, personal lending, savings, investments, credit card services and more

Employees: 665

Members: 450,000

Total Assets (2007): € 19.5 billion

THE IRONPORT ADVANTAGE

- Accurate detection and classification of illicit images and content
- Minimized exposure to legal liability as well as loss of brand image and reputation
- Easy management with maximum visibility into acceptable use policy violations
- Complete integration with content filtering and reporting infrastructure



Overall, IronPort Image Analysis has been a very useful product. Prior to deployment, we relied on manual detection of unwanted attachments. This was a major drain on productivity and continually posed the risk of allowing inappropriate content to breach the internal network. IronPort has enabled a significantly more robust monitoring process. ”

— David Cahill, Information Security Specialist
EBS Building Society



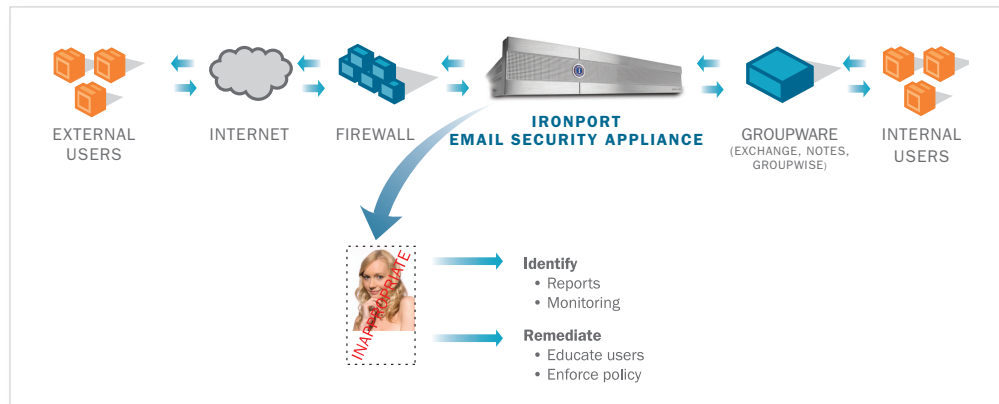
THE SITUATION

With a trusted brand built on a long history of providing quality products and service, EBS Building Society is one of Ireland’s most respected financial organizations. However, in recent years, the proliferation of illicit email-borne images posed a serious threat to its hard-earned market stature as well as the safety and security of its employees and members. Based on its satisfaction with its existing IronPort C-Series™ email security appliance, the organization looked to IronPort® for a new means to combat these increasingly complex threats.

TECHNICAL CHALLENGES

With roughly 1,200 users on its system, EBS realized that manual detection of suspect images was an unsustainable proposition given the drain on productivity and probability for human error (which continually posed the risk of allowing inappropriate content to infiltrate its network). The company needed a more efficient means to analyze the threats posed by external users who create, upload and share inappropriate images. Employers are required to provide a safe work environment for their employees, and block message content that can compromise their brand identity or reputation in the market. With that in mind, EBS sought a powerful resource that would accurately identify inappropriate content at the gateway, and maintain it in quarantine until its risk could be evaluated. After a rigorous two-month trial, EBS selected IronPort Image Analysis.

IronPort Image Analysis uses state-of-the-art technology to detect illicit content in both incoming and outgoing email – allowing customers to identify, monitor and educate offending users.



THE IRONPORT ADVANTAGE

The distribution of problematic images via email, particularly offensive graphics, jeopardizes organizations worldwide. IronPort Image Analysis has emerged to help ensure enterprises’ enforcement of acceptable use policies and ultimately preserve the integrity of their reputation in the marketplace.

Integrated into the award-winning IronPort C-Series appliance, the IronPort Image Analysis solution has enabled EBS to prevent illicit images from entering its network, identify traffickers, and dramatically reduce the amount of time spent protecting the network from such threats.



The system draws on 11 different detection methods to render a verdict on suspect attachments and easily configurable settings that give administrators full control to determine what actions to take on a particular message. Additionally, embedded image scanning enables a rigorous inspection of attached and embedded files – such as JPEG, BMP, PNG, TIFF, GIF, TGA, ICO and PCX. IronPort's scanning engine can extract images from more than 400 file types, including Word, Excel and PowerPoint.

IronPort Image Analysis is easily aligned with message and content filters to readily allow policy-based filtering and reporting on senders and recipients. When an illicit image is detected within email, a variety of actions can be taken – including stripping the attachment from the message or stamping it with a company policy message. EBS was particularly pleased with the technology's ability to remove a suspect image from a message, while still allowing the message's text to be delivered to its intended recipient.

EBS estimates that approximately 40 percent of all email traffic attempting to enter its network contains inappropriate image content. Since deploying IronPort Image Analysis, the company reports that 99 percent of that bad content has been blocked. The management time allocated to combat this problem has also been dramatically reduced from several days per week to only a few hours. IronPort enables EBS to protect its users and itself.



IronPort Systems

950 Elm Avenue, San Bruno, California 94066

TEL 650.989.6500 FAX 650.989.6543

EMAIL info@ironport.com WEB www.ironport.com

IronPort Systems, now part of Cisco, is a leading provider of anti-spam, anti-virus and anti-spyware appliances for organizations ranging from small businesses to the Global 2000. IronPort appliances utilize SenderBase, the world's largest email and Web threat detection network and database. IronPort products are innovative and easy-to-use—providing breakthrough performance and playing a mission-critical role in a company's network infrastructure.

Copyright © 2000-2008 Cisco Systems, Inc. All rights reserved. IronPort, the IronPort logo and SenderBase are registered trademarks of Cisco Systems, Inc. All other trademarks are the property of Cisco Systems, Inc. or their respective owners. While every effort is made to ensure the information given is accurate, Cisco does not accept liability for any errors or mistakes which may arise. Specifications and other information in this document may be subject to change without notice. P/N 451-0149-1 7/08

IronPort is now
part of Cisco.

